Office of Information Security

Secure Coding Tips

Scan issues must be audited inside Fortify per VA Secure Code Review SOP

This week's Secure Coding Tip is about the method by which HP Fortify Static Code Analyzer (SCA) scan issues must be audited per VA Secure Code Review Standard Operating Procedures (SOP).[1] Scanning source code to perform code review is an authorization requirement included in the Technical / Testing Requirements of the OCS Accreditation Requirements Guide / SOP [2] , and enforced as part of the ATO issuance process.[3]

HP Fortify SCA scan issues must be audited per VA Secure Code Review SOP inside Fortify, as opposed to outside for example in a text document or in a spreadsheet.[4] While it is acceptable to provide additional details for some complex issues in an external document (such as a design document), there still must be audit comments in Fortify and those comments must then reference the external document.

Read more...

[1] VA Secure Code Review SOP
[2] "Accreditation Requirements Guide / Standard Operating Procedures", Office of Cyber Security (OCS) Assessment and Authorization intranet site.
[3] "Accreditation Requirements Expectation Memorandum" (Section 2.a.ii "Code Review"), VA Chief Information Security Officer (CISO) Stanley F. Lowe, March 19, 2014.
[4] VA Top 10 Fortify Scan Issues For 2016 (Q1), S9: Audit was not performed within Fortify

More Information

For more information about the VA Software Assurance Program Office, please visit our website here.

Resources

Request VA-licensed code review tools, validations, and support here

Latest VA Software Assurance Program Office announcements can be found here

Learn more about VA code review processes here

Next Class:
2/23

VA Working Group Registration Instructions

VA Application Registration Instructions

Next Working Group Meeting:
2/8